GENERAL DYNAMICS
C4 Systems

General Dynamics
Secure Virtualization Solutions

Chuck Roose
Principal Systems Engineer
Information Assurance Division

Virtualization Security Characteristics

- **Separation/Isolation**
  - Independent Virtual Machines
  - Independent “Virtual Appliances”
  - Isolate Vulnerabilities
  - Limit Attack Vectors
- **Virtual Machine Monitor (Hypervisor)**
  - Security “Control Point”
  - Memory Management
  - Enables Audit
- **Fail Safe**
  - Fast, efficient recovery from failures
  - Redundant Processes

Enablers

- **Hardware Virtualization and Security Features**
  - Intel VT
  - Intel TXT
  - Trusted Platform Module (TPM)
- **Software Virtualization and Security Features**
  - Virtualized Access to Peripherals
  - Memory Management
  - Process Containment
- **Open Standards from Trusted Computing Group**
  - Trusted Network Connect (TNC)
  - TPM
  - Other (Virtualization Standards, PC Client,…)

Trusted Virtual Environment – An application of secure virtualization

Trusted Virtual Environment (TVE), High Assurance Platform-compliant: A partnership between the U.S. Government, General Dynamics, and industry leaders, where one computer simultaneously runs multiple operating systems in different security domains

Multiple Form Factors

Brings multi-level and cross-domain computing to tactical and strategic environments using a single low-cost COTS computer, standard operating systems, and existing applications

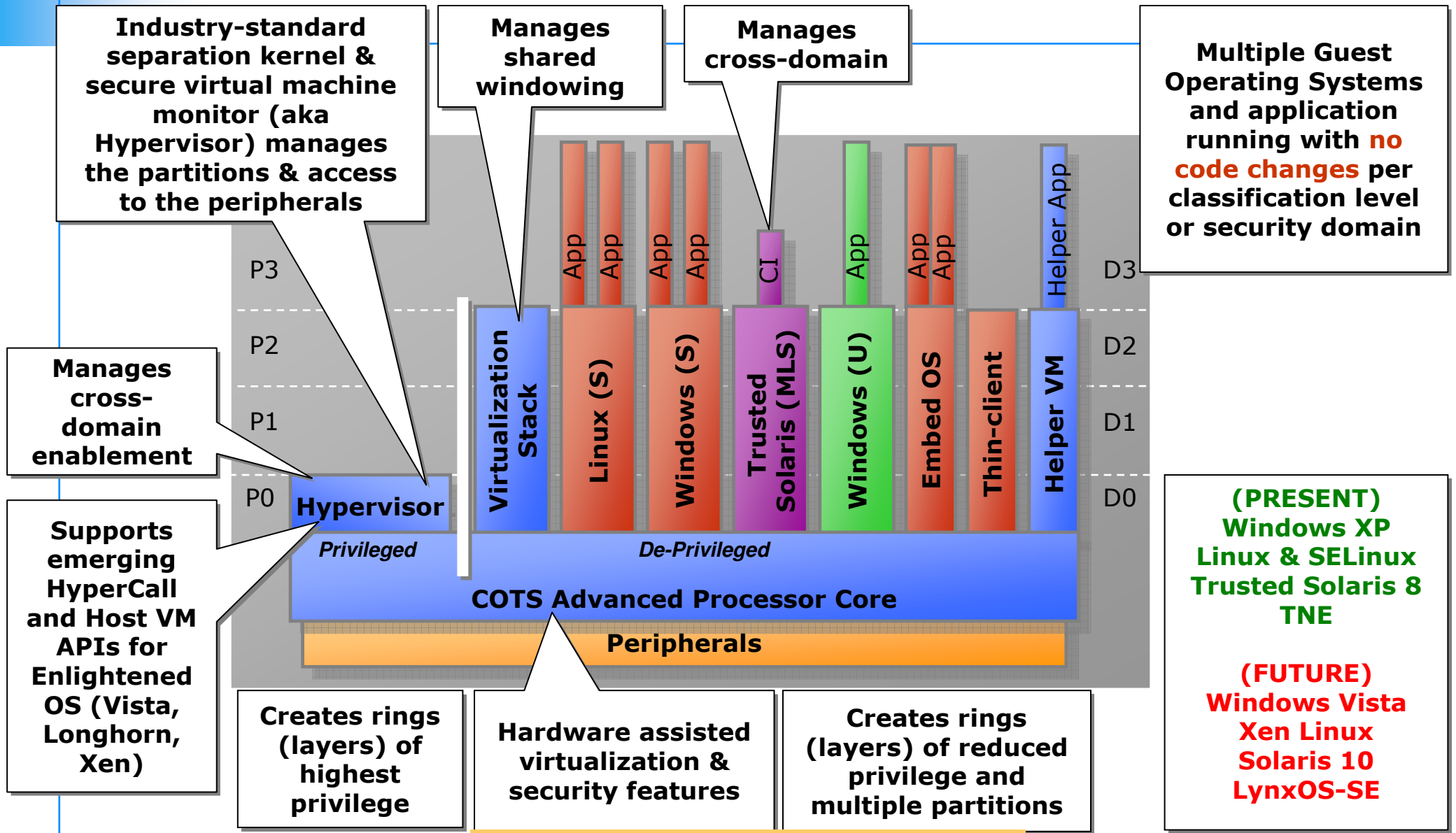
Empowers "Assured Information Sharing" across multiple U.S. or Coalition security domains without needing extensive classification labelling

Drives reduction in hardware size, weight, and power, and number of networks needed

"Commercial HAP-Compliant Solution"

Note: security classification labels in this briefing are for example purposes and DO NOT reflect any actual classification; all information in this brief is unclassified.

TVE Architectural Approach



G.H.O.S.T.TVE Team and Partners

GHOST TVE Trusted Virtual Environment

INDUSTRY PARTNERS

GENERAL DYNAMICS C4 Systems — Integrator and High Robustness Software

intel — COTS Security Enhanced Platform

vmware — COTS Virtualization Software

LYNUXWORKS — Integrator and High Robustness Software

DolphinTechnology, galois, KESTREL — Formal Methods and CDS Tech Providers

DELL — Hardware provider

Industry Memberships

TRUSTED COMPUTING GROUP

PCI SIG

Technology Integrations

Microsoft, redhat, CISCO, Sun microsystems, Juniper NETWORKS

GOVERNMENT PARTNERS

U.S. National Security Agency — HAP Program Manager, IA Oversight, Certification

Operational Sponsors, Accreditation Sponsors, Technology Providers

- U.S. Special Operations Command
- U.S. Pacific Command
- U.S. Defense Intelligence Agency
- Canada Dept of National Defence
- U.S. Air Force Research Lab
- U.S. NSA IA Research Lab (National Information Assurance Research Laboratory)
- U.S. Navy

Questions?

General:
(866) 400-0195
IASystems@gdc4s.com

TVE / HAP: Chuck Roose
(813) 314-8776
Chuck.Roose@gdc4s.com

Service & Support:
(877) 230-0236
infosecsupport@gdc4s.com

International: +1 (410) 850-4893
DSN: 644-1139